HP StorageWorks HA-Fabric Manager release notes

Part number: AA–RUR6F–TE/958–000288–010
Eighth edition: Aug ust 2005

Legal and notice information

Printed in the U.S.A.

HP StorageWorks HA-Fabric Manager release notes

About this document

These release notes describe the contents of the HAFM software kit, and any last-minute additions or notes on the configuration or use of HAFM software.

Be sure to read these notes before installing the HAFM. This information is periodically updated and available on the following HP web site: http://www.hp.com/country/us/eng/prodserv/storage.html.

This section describes the content reflected in this document, including:

- Release notes information
- Intended audience
- Other HAFM documentation
- CDROM directory structure
- HAFM software version 08.06.00
- Important information
- Known issues

Release notes information

These release notes cover the following major topics:

- Setting date/time of HAFM appliance to earlier time may cause loss of management to switches
- HAFM installation not correctly cancelled by ESC key or Space bar
- Performance graphs inaccurate for time period when HAFM appliance is shut down
- FL Ports do not show Destination icon or Destination port in performance graphs
- Changing or removing the principal switch of a persisted fabric causes two fabrics to be displayed
- Removing a Port Fencing Threshold Policy may not occur as expected under specific conditions
- Port Fencing dialog box may not reflect correct count of Affected Ports in ISL Thresholds table
- User-defined nicknames for node devices do not show in Connection Properties
- Port WWN is listed in the Node WWN field of Properties dialog box of a node device
- Error message window may display after you close the HAFM application
- Modem-based Call Home Configuration icon still appears after LAN-based Call Home is installed
- Ethernet port failure on HAFM appliance may impact HAFM behavior
- AIX client may not connect to HAFM appliance

Intended audience

This document is intended for customers who purchased HAFM. HAFM 08.06.00 applies to the 1U rack-mount appliance only and cannot be installed on the notebook server.

Other HAFM documentation

In addition to these release notes, HP provides the following corresponding information:

- *HP StorageWorks HA-Fabric Manager Appliance Installation Guide*, AA-RU5FC-TE/958-000324-002
- *HP StorageWorks HA-Fabric Manager User Guide*, AA-RS2CF-TE
- *HP StorageWorks HA-Fabric Manager Transition Guide*, AA-RV1MB-TE/958-000384-001
- *HP StorageWorks Director and Edge Switch Glossary*, AA-RU5JB-TE
- *HP StorageWorks C-FCSWAPI SDK Bridge Agent Installation Instructions*, AA-RVJ1B-TE/958-000405-001

CD-ROM directory structure

The HAFM software kit includes two CDs; the HP StorageWorks ha-fabric manager documentation and software CD (part number 516-000008-000, Rev A) and the HP StorageWorks ha-fabric manager clients CD (part number 516-000009-000, Rev A), which contains the files necessary to install HAFM.

The HP StorageWorks ha-fabric manager documentation and software CD contains the following items at the root level directory:

- Open_Bridge_Agent_Installer—Directory for installer
  - `version.txt`—File used for installer
  - `copyright.txt`—File used for installer
  - `BridgeAgentInstall.exe`—File used for installer
- HAFM82_win—Directory for init file
  - `data1.cab`—File used for HAFM installation
  - `data1.hdr`—File used for HAFM installation
  - `data2.cab`—File used for HAFM installation
  - `HAFM.ico`—File used for HAFM installation
  - `ikernel.ex_`—File used for HAFM installation
  - `layout.bin`—File used for HAFM installation
  - `setup.bmp`—File used for HAFM installation
  - `setup.exe`—Install file for HAFM applications
  - `Setup.ini`—File used for HAFM installation
  - `setup.inx`—File used for HAFM installation
  - `Uninstall.ico`—File used for HAFM installation
  - `version.txt`—Contains the version number of the HAFM Applications
- Documents
  - `README.TXT`—HP document structure; late-breaking doc changes
  - `COPYRIGHT.TXT`—Contains the copyright information
  - AA-RU5FC-TE/958-000324-002—*HP StorageWorks HA-Fabric Manager Appliance Installation Guide*
  - AA-RS2CF-TE—*HP StorageWorks HA-Fabric Manager User Guide*
  - AA-RV1MB-TE/958-000384-001—*HP StorageWorks HA-Fabric Manager Transition Guide*
  - AA-RU5JB-TE—*HP StorageWorks Director and Edge Switch Glossary*
  - AA-RVJ1B-TE/958-000405-001—*HP StorageWorks C-FCSWAPI SDK Bridge Agent Installation Instructions*

The HP StorageWorks ha-fabric manager clients CD contains the following items at the root level directory:

- AIX
  - hpClientInstall.bin
- HPUX
  - hpClientInstall.bin
- Linux
  - hpClientInstall.bin
- Solaris
  - hpClientInstall.bin
- Windows
  - hpClientInstall.exe
- version.txt
- Documents
  - `README.TXT`—HP document structure; late-breaking doc changes
  - `COPYRIGHT.TXT`—Contains the copyright information

HAFM software version 08.06.00

The HAFM appliance has the latest version of the HAFM software pre-installed. It is also contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000008-000, Rev A). HAFM 08.06.00 applies to the 1U rack-mount appliance only and cannot be installed on the notebook server.

All remote clients running down-level versions of HAFM are required to reinstall the client application. You must exit HAFM before installing the latest version of HAFM. When logging in to the HAFM appliance via the remote client, an error message is displayed stating that the new version must be installed. Follow the instructions to install the new version of the remote client.

Upgrading to HAFM 08.06.00 issues

The password for the Administrator must be reset to "password" before upgrading. If this is not performed before upgrading, the HAFM appliance may stop immediately after starting it.

Upgrading to HAFM 08.06.00 from 08.02.00 requires HAFM Services to be stopped manually.

The password for HAFM Administrator does not migrate from HAFM 07.xx.xx to HAFM 08.06.00. The password is reset to the default value, "password" in HAFM 08.06.00.

Call Home configuration is not migrated from HAFM 08.02.00 to HAFM 08.06.00 during upgrade. The Call Home information must be configured again after the upgrade.

Configuration information for switches that are not being managed locally are not included in the upgrade.

Firmware files are included in the upgrade process, but release rules are not. Since release rules are required when sending another firmware version to a switch, an error results. To avoid this problem, add the latest firmware file to the firmware library. This also adds the new release rules and resolves the problem.

HAFM 07.02.00 is not removed after upgrading to HAFM 08.xx.xx, and if the server is rebooted, both 07.xx.xx and 08.xx.xx services are started. Be sure to remove 07.02.00 after upgrading to 08.xx.xx.

Important information

This section describes important information related to the HAFM software, the Edge Switch 2/24, Edge Switch 2/32, Director 2/64, and Director 2/140.

Features not supported in this release

The following director and edge switch feature is not supported in this release:

- SANtegrity Authentication

The following HAFM features are not supported in this release:

- SANtegrity Security Center
- Group Configuration Manager

These features are described in the documentation released with firmware 07.00.00 and HAFM 08.06.00. Some of these features may be available in a future release.

Documentation released with firmware 07.00.00 and HAFM 08.06.00

To support these products, we are providing documentation from both McDATA Corporation (the product developer) and from HP (the product OEM). The HP documents include all information HP has incorporated into the products to date. The McDATA documents include only the basic product information.

Table 1 shows HP terminology and McDATA Corporation equivalents used in the McDATA documents.

Table 1 HP and McDATA terminology

HP term	McDATA term
HP StorageWorks Edge Switch 2/12	Sphereon 4300 Fabric Switch
HP StorageWorks Edge Switch 2/16	Sphereon 3216 Fabric Switch
HP StorageWorks Edge Switch 2/24	Sphereon 4500 Fabric Switch
HP StorageWorks Edge Switch 2/32	Sphereon 3232 Fabric Switch
HP StorageWorks Director 2/64	Intrepid 6064 Director
HP StorageWorks Director 2/140	Intrepid 6140 Director
Embedded Web Server (EWS)	SANpilot
HA-Fabric Manager (HAFM)	Enterprise Connectivity Manager (EFCM)
Firmware	Enterprise Operating System (E/OS)
HAFM Appliance	EFC Server

Formatting is required for new backup CD-RW disks

If you use a different CD-RW disk to backup other than the one provided with the HAFM appliance, you must access the desktop of the HAFM appliance in order to enable the formatting of the new disk. Backups cannot be performed until the new disk is formatted.

Upgrading from previous HAFM versions requires a special process

If you have an HAFM notebook server or an HAFM appliance and you are upgrading to HAFM 08.06.00, you must follow the directions as detailed in the *HP StorageWorks HA-Fabric Manager Transition Guide*, to successfully transfer your SAN configuration information to HAFM 08.06.00.

HAFM 08.06.00 improvements

The *HP StorageWorks HA-Fabric Manager Transition Guide*, shipped with the product, explains upgrading HAFM from an earlier version.

HAFM and firmware compatibility

Table 2 lists the minimum version of HAFM that can run with the various versions of firmware for the directors and edge switches. HAFM 08.06.00 allows managing of directors and edge switches running any of the versions of firmware listed in Table 2:

Table 2 HAFM and firmware compatibility

Firmware version	HAFM version (minimum)
01.01.02	04.00.01 (HP EFCM)
01.02.02-06	04.01.02-14 (SDCM)
01.03.00-35	04.02.00-40 (HP EFCM)
01.04.00-01	04.02.00-40 (SDCM)
02.00.00-33	06.00.00-45 (HP EFCM)
02.00.02-01	06.00.02-06
04.01.02-04	06.03.01-05
05.02.00-13	07.01.00-09 (Notebook Server)
05.02.00-13	07.02.00-09 (HAFM Appliance)
05.05.00-12	None (Edge Switch 2/12)
06.01.00-18	07.01.00-09 (Notebook Server)
06.01.00-18	07.02.00-09 (HAFM Appliance)
06.01.00-18	08.02.00 recommended (HAFM Appliance)
06.02.00-22	07.01.00-09 (Notebook Server)
06.02.00-22	07.02.00-09 (HAFM Appliance)
06.02.00-22	08.02.00 recommended (HAFM Appliance)
07.00.00-84	07.01.00-09 (Notebook Server)
07.00.00-84	07.02.00-09 (HAFM Appliance)
07.00.00-84	08.06.00 recommended (HAFM Appliance)

Prerequisites for installing and using firmware 07.00.00

If you are using HAFM, firmware 07.00.00 requires HAFM 07.01.00 or later (check with HP Customer Support for the latest shipping version of HAFM). HAFM should be at the minimum level before installing the new firmware.

NOTE:

HAFM is not required for operating hardware products using the firmware.

All directors and edge switches in the same fabric should have the same firmware level installed. Although products may coexist in a fabric running different levels of firmware, all products *must* be at the same major functional release level.

HAFM upgrade required for firmware version 07.xx.xx

To upgrade to firmware 07.00.00-84, you must first upgrade the HAFM software to 07.01.00-9 minimum, if you are using the notebook HAFM server to manage the director or edge switch. The HAFM software is contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000024-820). An upgrade kit to HAFM 07.01.00-9 is also available, Part Number 320908-B22, for owners of license for previous versions. This HAFM upgrade is also available on the following HP web site: http://h18006.www1.hp.com/storage/saninfrastructure.html

If you are using the 1U rack-mount HAFM appliance to manage the director or edge switch, the minimum HAFM version required is 07.02.00-9, which is the minimum version installed. This HAFM software is contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000024-720).

The previous minimum versions of HAFM allow you to manage directors or edge switches running 07.00.00-84 firmware, but to be able to use all the new features and enhancements, you need to upgrade HAFM to 08.06.00, which runs only on the 1U rack-mount HAFM appliance.

As an alternative, you can perform the firmware upgrade directly to the director or edge switch using their EWS.

Please contact your local HP technical resource if you need to obtain a new HAFM version.

Please contact your local HP technical resource to confirm compatibility with devices in your SAN before upgrading to this firmware version.

For more information on upgrading software versions, refer to the *HP StorageWorks HA-Fabric Manager User Guide*. The features of this software version are detailed in the accompanying manuals listed in section Other HAFM documentation.

Upgrading from an earlier version of firmware

Upgrading to firmware 07.00.00-84 is non-disruptive to attached devices. The director or edge switch is not required to be offline before performing an upgrade operation. Limitations to upgrades are clearly identified if there are any limitations to performing the operation.

Before upgrading firmware, it is highly recommended that you back up the director or edge switch configuration. Refer to your HP StorageWorks director or edge switch

Element Manager user guide for more information. Embedded Web Server (EWS) also provides an option to print or save product configuration to a file. Refer to the *HP StorageWorks Embedded Web Server User Guide* for more information.

All products must be running firmware 06.00.00 or later before upgrading to 07.00.00-84. If a switch is operating with a firmware level earlier than 06.00.00, you must upgrade to 06.xx.xx before installing 07.00.00-84.

Upgrades and downgrades are supported only from one major release to the next, such as from 06.xx.xx to 07.00.00-84. If EWS is used for upgrades and downgrades, and this rule is not followed, errors occur and there may be a disruption to attached devices.

If upgrading to firmware 06.02.00-22 requires you to upgrade from 04.xx.xx to 05.xx.xx in the process, there are special considerations:

- For directors, refer to Upgrading firmware on a director from 04.xx.xx to 05.xx.xx
- For edge switches, refer to Upgrading firmware on an edge switch from 04.xx.xx to 05.xx.xx

A small number of early-shipped Surestore Director FC-64 units may receive one of the following messages when they upgrade to firmware 05.02.00-13:

- `HAFM`—Firmware cannot be loaded due to insufficient CTP memory.
- `EWS`—File System Error: Insufficient memory for new firmware version.

This occurs only in certain units with CTP cards. Units with CTP2 cards do not have this issue.

If you get one of these messages during the upgrade, the firmware upgrade failed, but the unit continues working with the existing firmware without an interruption in service. The upgrade process checks for sufficient memory before activating the new firmware image. The firmware upgrade does not complete without sufficient memory. Please contact HP Customer Support if you receive this message.

Some customer environments use application or host software that is affected by the restart of the director CTP during a HotCAT download operation. Applications that rely on inband management servers are especially prone to problems caused by processor restart. For example, an application may be configured to poll the director or switch at regular intervals. The polling process could occur during a restart period, causing the application software to react adversely. As a solution, shut down those applications driving inband requests during a firmware upgrade, then restart the applications after upgrade completion.

Upgrading firmware on an edge switch from 04.xx.xx to 05.xx.xx

An issue has been identified in release 04.xx.xx if the contents of the nonvolatile storage (NVRAM) on the CTP become corrupted. Once the configuration has been loaded, this corruption is not detected until an IPL/IML, power cycle, or firmware code load. If the NVRAM in the CTP has corrupted contents, the firmware load can cause the configuration to reset to factory defaults, which could cause a system outage.

Edge switch products already running 05.01.00 or later continually validate the NVRAM configuration, so risk of an outage is extremely low. For edge switch products running an earlier version of firmware, the risk of an outage increases due to the NVRAM issue. If an outage compromises system integrity, HP recommends that the edge switch firmware upgrade be a scheduled maintenance action that anticipates the failure of switch connectivity. This issue was corrected with firmware 05.02.00-13 and later.

To safely upgrade firmware on a edge switch, perform the following:

1. Upgrade HAFM software on the HAFM server/appliance to 07.01.00 (minimum).
2. Download firmware 05.02.00-13 using the **Firmware Library** option under the Product Manager Maintenance menu.
3. Back up the edge switch configuration using the **Backup & Restore Configuration** option under the Product Manager Maintenance menu.
4. Upgrade the firmware to 05.02.00-13 on each edge switch using the **Send** option on the Firmware Library dialog box.

Upgrading firmware on a director from 04.xx.xx to 05.xx.xx

An issue has been identified in release 04.xx.xx if the contents of the nonvolatile storage (NVRAM) on the active CTP become corrupted. Once the configuration has been loaded, this corruption is not detected until an IPL/IML, power cycle, or firmware code load. If the NVRAM in the active CTP has corrupted contents, the firmware load can cause the configuration to reset to factory defaults, which could cause a system outage. By using the following procedure to upgrade firmware, configuration is preserved and a system outage is avoided. This issue was corrected with firmware 05.02.00-13 and later.

NOTE:

Step 4 of the following procedure is not required if you are upgrading from 05.xx.xx or later.

To safely upgrade firmware on a director, perform the following:

1. Upgrade HAFM software on the HAFM server/appliance to 07.01.00 (minimum).
2. Download firmware 05.02.00-13 using the **Firmware Library** option under the Product Manager Maintenance menu.
3. Back up the director configuration using the **Backup & Restore Configuration** option under the Product Manager Maintenance menu.
4. Using the Product Manager, execute a CTP swap:

NOTE:

You must have maintenance authorization rights to access the HAFM Product/Element Manager menu options used in this procedure.

a. From Product/Element Manager Hardware view, verify that an amber LED indicator is not displayed for either CTP card.
b. Right-click the CTP card you believe to be active. From the right-click popup menu, choose **FRU Properties**. Verify that it is the active CTP card.
c. Right-click the active CTP card and choose **Switchover** from the popup menu.

   The director loses its Ethernet connection for a short period during the switchover process.

   When switchover occurs, the green LED illuminates on the backup CTP card to indicate that it is now the active card.

5. Upgrade the firmware to 05.02.00-13 on each director using the **Send** option on the Firmware Library dialog box.

Considerations for downgrading the version of firmware

Directors or edge switches are not required to be offline before performing a firmware downgrade operation. Limitations to downgrades are clearly identified if there are any limitations to performing the operation.

Before downgrading firmware, it is highly recommended that you back up the director or edge switch configuration. Refer to your HP StorageWorks director or edge switch Element Manager user guide for more information. EWS also provides an option to print or save product configuration to a file. Refer to your *HP StorageWorks Embedded Web Server User Guide* for more information.

Before downgrading below 07.00.00-84, there can only be one user assigned access rights as Administrator and one user assigned as Operator for Embedded Web Server and CLI. If additional users were created, you have to delete them before downgrading. Firmware 07.00.00-84 does not allow the last user with Administrator rights in Embedded Web Server or CLI to be deleted. If no Operator user exists, firmware 07.00.00-84 automatically creates one for each interface during the downgrade. If more than one Administrator and/or one Operator exists for Embedded Web Server and/or CLI, when attempting to downgrade you are prompted to delete one of them first.

When downgrading to a release prior to 07.00.00-84, any modifications to the port RX BB_Credit settings using the new enhanced port configuration capability must be changed back to a configuration supported by older firmware. This is necessary to allow the configuration to comply with previous releases' configuration database. Firmware 07.00.00-84 services verify compatibility and prevent downloads until the configuration conflict is resolved.

For procedures to download firmware to the switch or director using the HAFM Element Manager interface or EWS interface, refer to the following:

- The switch or director Installation and Service Manual. This publication provides complete procedures for obtaining firmware from the HP web site and downloading firmware to the switch or director using HAFM.
- The switch or director Element Manager online help and User Manual. These includes instructions for downloading firmware to the switch or director using the HAFM interface.
- EWS User Manual. This provides procedures for downloading firmware to the switch or director.
- EWS online help. This provides procedures for downloading firmware to the switch or director.

Downgrading directly to a release before 06.00.00 from 07.00.00-84 is not allowed. To downgrade to a release before 06.00.00, you must first downgrade to 06.YY.ZZ.

Upgrades and downgrades are supported only from one major release to the next, such as from 06.xx.xx to 07.00.00-84. If EWS is used for upgrades and downgrades, and this rule is not followed, errors occur and there may be a disruption to attached devices.

Downgrading to release 6.0 with the Preferred Path feature configured could cause loss of this function. HP recommends that Preferred Path be disabled before downgrading. To do this, deselect the check box for **Enable Preferred Path** in the Configure Preferred Paths dialog box.

NOTE:

The Director 2/140 and the Edge Switch 2/24 cannot be downgraded earlier than 04.01.00, and the Edge Switch 2/12 cannot be downgraded earlier than 05.05.00.

If a Director 2/140 in a multiswitch fabric is downgraded earlier than 06.02.00, ISLs could become segmented if there are any other switches in the fabric operating with a firmware version earlier than 06.01.00. To prevent this situation, downgrade all Director 2/140s in the fabric to 06.01.00 before downgrading any products in the fabric to 05.xx.xx. This problem only exists with Director 2/140s in the fabric. HAFM displays a warning message if a downgrade from 06.02.00 is attempted, but you can continue with the downgrade if desired.

NOTE:

The warning message is displayed when downgrading any model from 06.02.00, but only applies to downgrade operations for the Director 2/140.

Downgrades directly to 05.03.01 from 06.xx.xx is not concurrent when the second-generation Edge Switch 2/24 is configured in **Open Fabric** operating mode. In other words, downgrades in **Open Fabric** mode cannot be done with the second-generation Edge Switch 2/24 online without disrupting port operations. Since

second-generation Edge Switch 2/24 switches cannot be downgraded earlier than 05.03.01, they must be configured in **Homogeneous Fabric Interoperability** mode to remain concurrent. If this process is not followed, I/O through the switch may be significantly disrupted or stopped. Recovery for this situation is accomplished by reactivating the current zone set.

If you are installing a new or replacement second-generation Edge Switch 2/12 or Edge Switch 2/24 into an existing 05.xx.xx fabric, HP recommends that you downgrade the unit before installing it into the fabric.

Downgrading to 05.05.00 is supported only on first-generation Edge Switch 2/12 switches. Second-generation Edge Switch 2/12 switches can be downgraded only to 05.05.01. Second-generation Edge Switch 2/24 switches can be downgraded only to 05.03.01.

Firmware downgrades should not be performed using EWS and Internet Explorer 5.00.3315.1000x. If this operation is performed, the download operation may not complete and may eventually time-out leaving the switch with the previous version of firmware.

Logging out of Microsoft Windows after access to HAFM appliance is recommended

After you access the HAFM appliance desktop via a web browser using the TightVNC application, HP recommends that you log out of Microsoft Windows before disconnecting your web browser access. This prevents unauthorized access to the HAFM appliance by someone using the TightVNC application to access the HAFM appliance. When the new user attempts to log into the HAFM appliance, the Welcome to Windows screen is displayed, and a Windows user name and password are required to access the HAFM appliance Windows desktop. HAFM remote client access does not require the HAFM appliance to be logged in to Windows.

Zone FlexPar feature

Because zoning is managed on a fabric-wide basis, all switches and directors in the fabric must maintain the same zoning configuration. This configuration is maintained automatically through the Fibre Channel protocol.

To keep this information current, RSCN messages are sent through the fabric to inform attached devices when zoning changes occur, when devices become available, or when devices become unavailable. In the case where devices become available or unavailable, RSCNs are sent only to the devices in the same zone. Zoning changes, however, trigger RSCNs to be sent to all of the devices in the fabric. As fabrics grow larger and larger, the quantity of RSCNs from zoning changes can create congestion and disrupt devices, causing them to pause normal activity to determine the status of the other devices. This can occur even if the new device is not zoned to talk to the other devices in the fabric.

With the Zone FlexPar feature enabled, RSCN messages for a zoning change are handled like RSCNs for availability/unavailability changes. Specifically, RSCNs are

restricted to only those devices sharing at least one common zone with the device that changed. This way, only devices that are impacted by the change in connectivity receive RSCNs.

The Zone FlexPar feature is available in both Open Fabric 1.0 and Homogeneous Fabric 1.0 Interop modes, as well as in environments with loop-attached devices. In Homogeneous Fabric 1.0 mode, the default zone is treated like any other zone, and RSCNs are sent only to the affected devices if the default zone is enabled or disabled. A PFE key is not required for the Zone FlexPar feature, and it can be enabled or disabled through CLI for a specific switch. When upgrading to firmware 07.00.00 or installing a new switch with firmware 07.00.00 the feature is enabled by default, allowing it to work immediately. If the Zone FlexPar feature is not enabled on all switches in the fabric, the restricted RSCN distribution only applies for devices attached to switches with the feature enabled.

Enhanced SANtegrity Security Suite

SANtegrity Security Suite enhanced features include authentication support for device login, interswitch connections and management interfaces. The Secure Access features are included as a standard part of the SANtegrity Security Suite in firmware 07.00.00.

Standard features

The following SANtegrity features do not require a license or SANtegrity Binding.

- **CHAP Authentication for HAFM/SWAPI**—This provides authentication of connections from the HAFM appliance service processor and SWAPI Direct Connect. This ensures that requested HAFM management sessions or SWAPI Direct Connect sessions are from a trusted source.
- **Encryption of Passwords and Secrets Shared with HAFM**—All secrets and password information are passed in encrypted format for greater security. This prevents "snooping" of Ethernet connection to capture user login and authentication secret information.
- **RADIUS Server Support**—This provides support for IETF RADIUS (Remote Authentication Dial In User Service) protocol for password authentication. Firmware 07.00.00 allows users to configure settings for using a RADIUS server. RADIUS provides centralized authentication services for multiple devices on a network. This means that several switches can be configured to use a single RADIUS server.
- **Prompted Change of EWS and CLI Passwords from Default**—This prompts users to modify the password settings for both the CLI and EWS interfaces the first time they log in using either of these interfaces.
- **RBAC Phase I: Enhanced User Rights Configuration**—RBAC is role based access control. This is the first phase of more comprehensive role-based access control planned for the CLI and EWS interfaces. Multiple users can now be configured for EWS or CLI, or both, through either interface. This allows users to configure additional user name/password combinations.

- **SSH for CLI**—Secure Shell (SSH) provides an encrypted connection, as an alternative to Telnet, to secure CLI access to switches and directors.
- **Enhanced Maintenance Port Security**—This allows users to enable enhanced authorization on the maintenance port, which is the switch or director RS-232 connection. Enhanced Authorization mode enforces stronger security policies, requiring users to change the well-known password to a case- sensitive private password the first time they use the maintenance port. Subsequent access by service personnel will require log in through the private customer-level access.

- **Security Log**—The Security Log is a new log available in EWS, CLI, and HAFM that records various events concerning integrity of a switch. This includes authorization or authentication problem detection, and approved and invalid access attempts. Each log entry provides an event number or reason, a date/time stamp, a trigger level (a type of security event severity), an event count, and a category and data pertaining to the specific event. The log wraps at 200 entries. This log provides customers with details to track down attempted security threats and identify the source of problems that might jeopardize the switch integrity.
- **IP Access Control List**—This allows users to establish a list of IP addresses from which the switch is allowed to accept connections. This prevents users who have access to the Ethernet LAN from attempting to access the Fibre Channel switches. Connection attempts from unauthorized IP addresses are ignored by the switch, making it appear that no device is connected. This is primarily intended for environments that are not on a private, inaccessible subnet, such as when installed in most cabinet configurations with a dual-NIC HAFM appliance Processor.

Advanced Fabric Diagnostics

This provides tools to monitor the fabric and identify potential problems before they impact network and application performance. Tools include ISL Fencing, new switch-centric Fabric and Embedded Port Logs, an Audit Log for the embedded user interfaces, and access to the Digital Diagnostic capabilities included with newer SFP transceivers.

ISL fencing

Also called Port Fencing, this feature allows customers to set up policies for blocking an ISL when problems occur that cause an ISL to "bounce" or repeatedly attempt to establish a connection. Any time an ISL is brought up or down, a fabric rebuild occurs, which can cause disruption in some environments. ISL Fencing will lessen the likelihood of having a problematic ISL connection disrupt a SAN.

To configure this feature, users set policies with thresholds based on the number of port events occurring during a set time period. If a port generates enough events to exceed the policy threshold, the port is automatically blocked and the user is notified. Transmit and receive traffic is disabled until the user can investigate, solve the problem, and manually unblock the port.

Embedded Audit Log

The Audit log is a new log available through CLI and EWS. This is not the same Audit Log available through HAFM. The log records all configuration changes to the switch to provide data for analyzing problems caused by configuration changes.

Embedded Port Log

The Embedded Port Log is a new log that records all Fibre Channel traffic from or to the embedded port. This log is actually implemented as two logs, one that allows entry wrapping and one that stops adding entries when filled. The logs allow filtering based on Class F frames, as well as by port number, to isolate specific events or problems.

This feature is intended for advanced users to diagnose and troubleshoot traffic problems within a SAN. The Embedded Port Log is available via EWS, CLI, and HAFM.

Embedded Fabric Log

The switch-based fabric log records events related to the following services:

- Fabric Controller
- Path Selection
- Login Server
- Name Server

The Fabric log is actually implemented as two logs, one that allows entry wrapping and one that stops adding entries when filled. This log is intended to provide information for analyzing fabric and switch behaviors and problems. The Fabric log is available via EWS, CLI, and HAFM.

OSMS change

Open Systems Management Server (OSMS) is now available as a standard feature. OSMS can be enabled/disabled via EWS, Command Line Interface (CLI), and HAFM.

Default zone is disabled by default

The default zone on the director or edge switch is disabled by default. Zoning must be configured in order for any devices connected to the director to communicate.

Some IP addresses must be avoided

If you use HAFM to manage other M-Series Fabric directors and edge switches, when you select IP addresses for edge switches, directors, and for the HAFM appliance, do not use IP addresses in the following range:

192.168.0.0 through 192.168.0.255—This subnet is used internally to the HAFM appliance. Using an IP address in this range causes the call-home feature to function incorrectly.

Hard zoning

Hard zoning is a security enhancement introduced in firmware 05.01.00-24 that prevents ports from accessing devices outside their zones. Hard zoning is enabled

by default when using firmware 05.01.00-24 or greater and cannot be disabled. All HP-approved host bus adapters (HBAs) limit access to devices within their zones, so you will not see a change in fabric behavior unless you are using nonstandard HBAs. Hard zoning improves security against intruders that load nonstandard HBA drivers.

Hard zoning is compatible with legacy zone definitions, including World Wide Name (WWN) and port zoning. You can use your existing zones and zone sets without any changes. There are no changes to the zoning interfaces, so you do not need to modify your zone management practice, modify your documentation, or retrain Storage Area Network (SAN) administrators.

Hard zoning controls access at the ingress port. When a port attempts to send a frame to a destination outside its zones, the frame is blocked. A Class 2 frame is fabric rejected, and a Class 3 frame is dropped.

Zoning change RSCN control

Normally, when a zone set is activated, a fabric format domain Register State Change Notification (RSCN) is sent to all devices in the fabric. With firmware 05.00.00 or later, you can disable these RSCNs from being sent. This is done using the **Suppress RSCNs on zone set activations** check box on the Configure Switch Parameters dialog box.

This feature significantly changes the normal behavior of the fabric. Devices will have no warning when zones change and will not automatically update their zoning information. The ability to suppress RSCNs is disabled (check box is not selected) by default. This feature can be configured through HAFM, EWS, and CLI.

SNMP changes

Firmware 07.00.00-84 supports the following management information base (MIB) versions on all products:

- Fabric Element MIB: 1.1
- MIB-II MIB: RFC-1213, non-implemented sections are not included
- FCEOS MIB: 2.0
- SNMP Framework MIB: RFC-2271 (1997/09/30)
- FA MIB: 3.0
- FA MIB: 3.1

SNMP requests can be received in either 3.0 or 3.1 of the Fibre Alliance (FA) MIB, and the switch responds in the same version. The switch can also be configured to use a specific version for traps generated by the switch.

Zoning limitations

With firmware 06.00.00 and later, you have the ability to configure large zone sets, including up to 1024 zones and 1024 end ports in a single zone set. Table 3 shows the supported limits for the edge switches and directors.

Table 3 Zoning parameters supported limits

Zoning parameter	Maximum value
Number of zone members in a zone	2048
Number of zones in a zone set	1024
Number of unique zone members in a zone set	2048
Total number of zone members in a zone set (where a zone member can be in multiple zones)	4096
Characters per zoning name	32
Number of unique zone members in HAFM Zoning Library	2048
Number of zones in HAFM Zoning Library	1024
Number of zone sets in HAFM Zoning Library	64
Number of end ports	1024
Number of devices supported (including loop devices)	1024

Using the same firmware

All directors and edge switches in the same fabric should have the same firmware level installed—whether 1 Gbps or 2 Gbps capable, this firmware operates correctly.

The recently released Edge Switch 2/12 had an interim firmware specific for the Edge Switch 2/12, 05.05.00-12. This firmware cannot be used for any other edge switch or director. This interim version is compatible with the M-Series firmware 05.02.00-13 used for the rest of the M-Series fabric products. The firmware 07.00.00-84 is a common firmware for all the M-Series fabric products, including the Edge Switch 2/12.

Firmware 06.02.00-22 provides support for second-generation Edge Switch 2/12 and Edge Switch 2/24 switches. This is the minimum M-Series firmware supported on the second-generation Edge Switch 2/12 and Edge Switch 2/24.

For customers who want to add a second-generation switch to their existing SAN, but are not ready to upgrade their SAN from 5.x to 06.02.00, there is a downgrade firmware version for each of these edge switches which provides compatibility with a SAN running 05.02.00.

Firmware 05.03.01-01 is available for the Edge Switch 2/24, and firmware 05.05.01-01 is available for the Edge Switch 2/12. These versions are installed only on the Edge Switch 2/24 and Edge Switch 2/12, and only when these switches are placed in a M-Series SAN running 05.02.00 firmware. A copy of these versions of firmware, are contained on the HP StorageWorks edge switch documentation and firmware CD (Part Number 524-000001-005).

Reinstalling feature licenses

Feature licenses (or keys) must be reinstalled after performing a factory reset on a director to regain use of the licensed features (e.g., SANtegrity Binding).

CTP controls port lights

Port lights on the edge switch and director products are controlled by the CTP functionality. Certain activities such as firmware updates, IPLing the CTP, or switching over to the backup CTP (director) can cause these port lights to extinguish momentarily until control is reasserted by the CTP. The actual Fibre Channel traffic is not affected during these times.

BB_Credit Allocation for ports

Firmware 07.00.00 supports the ability to allocate a specific number of buffer credits per port. This feature provides benefit primarily in the Edge Switch 2/12 and 2/24 switches, where a single pool of buffers is shared among all ports. Users will now be able to allocate buffer credits only where needed. For the Director 2/64, Director 2/140, and Edge Switch 2/32 switches, this enhancement simply allows more granular configuration options for users who want complete configuration control.

NVRAM caching

All writes to non-volatile memory random access memory (NVRAM), which stores configuration data, are now cached to prevent possible corruption of information. Prior to firmware 07.00.00, a small window existed where a switch power-down during an NVRAM write could enable the configuration default settings when the switch is powered back on. All switches and directors are now protected from potential interruptions to NVRAM updates.

Robust large fabrics

Numerous low-level enhancements and optimizations have been made to improve the stability of directors and switches in fabrics containing high populations of devices.

Changing password in CLI

When users are prompted to change the password when logging into the Command Line Interface (CLI), they can enter the default password (password). This will be accepted, however at the next login they will again be required to change the password if it is still the default password.

When users enter the default password when prompted to change the password, new `Security Log entry 10203, Default Password Not Changed`, is posted.

Zoning enhancement to reduce fabric congestion

In Homogeneous Fabric mode, an enhancement was added to reduce unnecessary fabric congestion when performing fabric-wide zoning operations that impact the Default Zone. This enhancement limits the number of members allowed in the Default Zone to 64. When the firmware detects a zoning operation that would cause the member count in the Default Zone to exceed 64 (such as deactivating an active zone set that has more than 64 members), the operation is aborted and the user interface (HAFM 8.6 or EWS) displays the following message: `Zoning request denied: Operation will cause the Default Zone to exceed its limit of 64 members.`

NOTE:

This limit is disabled when the switch parameter **Suppress Zoning RSCNs on Zone set activations** check box is enabled.

Issue concerning HAFM remote client access to the HAFM appliance with dual LAN configuration

When using a single public LAN connection at the HAFM appliance for all Ethernet communications, the single LAN connection operates correctly for the following functions:

- Directors and edge switches that the HAFM appliance manages
- Computers seeking remote client access to the HAFM appliance
- SAN management applications such as HP OpenView SAN Area Manager

When using two LAN connections (public and private) at the HAFM appliance, Microsoft Windows and HAFM determine the following:

- Which LAN is to be the private LAN for communication between the HAFM appliance, and the directors and edge switches that the HAFM appliance manages?
- Which LAN is to be the public LAN for communication between the HAFM appliance and computers seeking remote client access to the HAFM appliance?

The issue arises because either LAN connection on the HAFM appliance can be the public LAN or the private LAN. Though the directors and edge switches can be

managed via either LAN, the public LAN is the only one that can support remote client access. Thus, if one attempts to access the HAFM appliance via a remote client session and is unknowingly using what has been designated as the private LAN, the remote session is not allowed. The IP address that the HAFM appliance has determined to be the public LAN which supports remote client access, displays HAFM which displays after selecting **SAN > Server Properties.**

HAFM designates the public LAN as the first LAN detected whose IP address is not the reserved private subnet `10.x.x.x`. Thus, if neither IP address is `10.x.x.x`, the first LAN detected by HAFM is designated as the public LAN. This order of detection is influenced by Microsoft Windows and is not guaranteed.

For a dual LAN configuration, both LANs must be connected when the HAFM appliance is booted up. If only one is connected, HAFM interprets this as a single LAN configuration, and the connected LAN is designated as the LAN for remote client sessions.

Workaround

There are a two ways to ensure the pubic and private designations of the LANs.

- If you use a private LAN IP address, this causes this LAN to be designated as the private LAN. You must also have the public LAN connection active when the HAFM appliance is booting up, or else HAFM interprets this as a single LAN connection configuration, and the `10.x.x.x LAN` is designated as the LAN for remote client sessions.
- You can configure a specified Ethernet interface on the HAFM appliance to be the public LAN (to listen for remote client connections). To configure this feature, you must manually edit a file on the HAFM appliance to explicitly specify which IP address HAFM should use as the public LAN.

  For detailed instructions, see *HP StorageWorks HA-Fabric Manager User Guide*.

  If the public LAN IP address of the HAFM appliance is ever changed, this file must be edited again to reflect the new IP address.

Known issues

This section describes the known issues related to the 1U HAFM appliance and the HAFM software.

Setting date/time of HAFM appliance to earlier time may cause loss of management to switches

When changing the HAFM appliance time to an earlier time, the Ethernet link to directors and edge switches may be lost, or an open element manager may close. When attempting to reopen the element manager, the error message “The link to the product is not available: Connection lost“ may be displayed.

Workaround

If the date/time of the HAFM appliance needs to be set to an earlier time, perform the following:

1. Exit the HAFM application.
2. Select **Start > Programs > HP StorageWorks ha-fabric manager 8.6 > Stop Services**.
3. Change the date/time on the HAFM appliance.
4. Select **Start > Programs > HP StorageWorks ha-fabric manager 8.6 > Start Services**.
5. Restart the HAFM application.

This procedure works even if you previously set the date/time to an earlier time without using these steps. Rebooting the HAFM appliance will also clear up this problem. Exiting the HAFM application or rebooting the HAFM appliance has no impact on the operations of the directors or edge switches and does not cause a disruption to fabric operations.

HAFM installation not correctly cancelled by ESC key or Space bar

During the HAFM application installation, the ESC key does not function to cancel the installation. The Space bar works only once to cancel the installation process.

Workaround

None. If the installation is not desired, allow the installation to complete and then uninstall the application.

Performance graphs inaccurate for time period when HAFM appliance is shut down

If the HAFM appliance has been shut down or the HAFM application and Services have been stopped, after restarting the performance graphs continue and draw a flat line from the stop point to the new start point. This indicates a level of performance during the down time but it is actually unknown. The reporting is inaccurate for that portion of the graph.

FL Ports do not show destination icon or destination port in performance graphs

FL Ports do not show destination switch icon or destination port in performance graphs. This is because there can be up to 127 devices on a loop port, and they cannot be displayed in the space in the tables.

Changing or removing the principal switch of a persisted fabric causes two fabrics to be displayed

Fabrics are identified by the WWN of the principal switch. If a new principal switch is selected (either manually, or because the current principal switch is removed from the fabric), the fabric is reidentified by the WWN of the new principal switch.

If the principal switch of a persisted fabric is changed or removed, two fabrics are displayed with identical switches, with the two fabrics identified by the former and the new principal switch WWN. The persisted fabric indicates all switches have been removed from fabric (red circle with minus sign) and all switch connections disabled (yellow dashed lines). The new fabric is not persisted.

Similarly, if the principal switch of a persisted fabric is removed from the fabric (ISLs removed or blocked) but still powered up and managed by HAFM, two fabrics are displayed with identical switches, with the two fabrics identified by the former and the new principal switch WWN. The persisted fabric indicates all switches except the former principal switch have been removed from fabric (red circle with minus sign) and all switch connections disabled (yellow dashed lines). The new fabric is not persisted.

Workaround

Unpersist the former fabric, and persist the new fabric.

Removing a Port Fencing Threshold Policy may not occur as expected under specific conditions

Under specific conditions, a Port Fencing Threshold Policy may remain active even if the user has removed it. This occurs when you are in the same Port Fencing configuration session:

1. A particular Port Fencing Threshold Policy is not currently applied to any switch.
2. The same Port Fencing Threshold Policy is applied to switch port(s).
3. The same Port Fencing Threshold Policy is selected in the ISL Threshold table (left panel), and **Remove** is clicked in order to remove this policy.
4. The Port Fencing configuration session is completed (by clicking **OK**).

Under these conditions, the Port Fencing Threshold Policy is not successfully removed and is active on the switch ports where the policy was applied.

Workaround

This can be corrected by repeating the selection of the Port Fencing Threshold Policy in the ISL Threshold table (left panel), by clicking **Remove**, and then clicking **OK**. The Port Fencing Threshold Policy will then be removed correctly. This can be avoided by also selecting the Port Fencing Threshold Policy on the switch ports where it was applied (right panel), and removing the policy from the switch port(s), before completing the session (step 4 above).

Port Fencing dialog box may not reflect correct count of Affected Ports in ISL Thresholds table

This usually occurs when a policy has been applied to an entire switch and there are already ports with a threshold policy applied, even when it is selected not to replace the existing policy on the switch ports.

User-defined nicknames for node devices do not show in Connection Properties

If you select **Show Route** between two node devices with user-defined Nicknames, the Nicknames for these nodes do not display in the Connection Properties when you double-click the route.

Port WWN is listed in the Node WWN field of Properties dialog box of a node device

When you right click on a node device in the Product List, and select **Properties** from the popup menu, the Properties dialog displays the Port WWN in the **Node WWN** field

Error message window may display after you close the HAFM application

An error message stating “Operation failed" may display after exiting an HAFM application which manages a large number of devices. This message is incorrect and should be ignored.

Modem-based Call Home Configuration icon still appears after LAN-based Call Home is installed

The Call Home Configuration icon that is used when the modem-based call home has been selected during HAFM installation, still appears when the LAN-based call home has been selected during HAFM installation. The Call Home Configuration icon also appears in the Windows Start menu:

Start > Programs > HP StorageWorks ha-fabric manager 8.6 > Call Home Configuration

Double clicking this icon or selecting this via the Windows Start menu when LAN-based call home has been selected produces the following error message: `Unable to access Call Home phone book - Please contact your service representative.` This has no impact on the functionality of the LAN based call home. Following the installation instructions for LAN based Call Home enables this function. There is no need to contact a service representative.

Workaround

If you installed the LAN based Call-Home feature, do not use the icon for Call Home Configuration or the Call Home Configuration icon that appears in the Windows Start menu.

Ethernet port failure on HAFM appliance may impact HAFM behavior

On the HAFM appliance, the SNMP agent may appear to hang or respond slowly if the Ethernet port on the server fails and transmits bad frames. CPU usage and memory usage display abnormally high.

AIX client may not connect to HAFM appliance

The remote client running on IBM AIX intermittently cannot connect to the HAFM appliance. AIX detects server when attempting login, but then displays a server not found and unable to connect message.

Workaround

If this issue is persistent, consider using an available HAFM client for another operating system.

Duplicate IP addresses erroneously allowed in Discover Setup Available Addresses list

The HAFM user is able to define a product with a duplicate IP address in the Available Addresses list on the Discovery Setup dialog box. However, the user is prevented from selecting two devices with the same IP address to be added to the Selected Individual Addresses list, so the potential conflict for managed devices is prevented.

Ethernet event may not be sent

An Ethernet event may not be sent for a switch that is in a discovered Fabric when the Ethernet cable is disconnected.

Domain IDs may not display

All Domain IDs that are in a 24 switch fabric may not display in the Product View.

SNMP traps are not displayed in the Event Log

SNMP traps that are sent through a firewall are not displayed in the Event Log.

Disconnected ISL may not generate Event Log entry

Log entries are not generated when a link between switches is disconnected. “Connection offline” and “Connection online” events are not created in the Master Log.

Cannot export to disk on remote AIX client

An exception is occurring when an export to disk operation is performed on a remote AIX client platform.

Cannot import a Physical Map

If an attempt is made to import a Physical Map by itself, the import fails.

Workaround

A Physical Map can be imported as part of a full SAN import file.

Errors drop down list is not available

The Errors drop down list is not available in the Performance Graph for HAFM 08.06.00.

Cannot configure a blank nickname

Nicknames cannot be left blank. If no nickname has been configured yet, the user can select cancel to leave a nickname blank. Once a nickname has been configured, it cannot be changed to be blank, that is, the nickname cannot be deleted. The nickname can be assigned a new name.

Support for speed Auto-Negotiate

Auto-negotiate is supported. However, HP recommends that the port speed for E_Ports (for Interswitch Links, or ISLs) be set to a specific port speed (**1Gb/sec** or **2Gb/sec**, as appropriate for the speed of the directors or edge switches being connected) instead of to **Negotiate**. Using a specific port speed decreases the time for a fabric build in response to some perturbation event in the fabric. Similarly, setting a specific port speed for N_Ports also decreases fabric build time. However, setting a specific port speed for N_Ports is not required.

There are a few older HBA devices that do not always succeed in logging in to a switch port when the port speed is set for auto-negotiate.

Workaround

If an older HBA has difficulty logging into a switch port that has its port speed configured as **Negotiate**, configure that port speed to **1Gb/sec** or **2Gb/sec** according to the operation speed of the HBA connected to that port.

Losing LAN connection to the HAFM appliance when logged in to HAFM

If the LAN connection to the HAFM appliance is lost while you are logged in to HAFM, the application may stop.

Workaround

The LAN connection must be restored. Stopping HAFM has no impact on the Fibre Channel operations of any edge switch or director. Monitoring switch operations, logging events, and implementing configuration changes are interrupted only while the LAN is not connected.

Effect of no LAN connection to HAFM appliance during boot up

If the HAFM appliance has no LAN connection while booting up, but it is connected after booting up, the remote client sessions to the HAFM appliance are not allowed. Also, the IP address that is displayed when you select **SAN > Server Properties** is possibly incorrect.

Workaround

This is corrected by restoring the LAN connection and rebooting the appliance. Rebooting the appliance has no impact on the Fibre Channel operations of any switch or director. Only monitoring switch operations, logging events, and implementing configuration changes are interrupted.

Setting HAFM appliance LAN to use DHCP is activated to wrong LAN

When setting the IP configuration for the HAFM appliance using the LCD panel, setting DHCP configuration for LAN 1 causes LAN 2, not LAN 1, to be configured for DHCP. Similarly, setting DHCP configuration for LAN 2 causes LAN 1, not LAN 2, to be configured for DHCP.

Workaround

If you wish to configure LAN 1 for DHCP, select LAN 2 instead of LAN 1 at the start of the configuration procedure. If you wish to configure LAN 2 for DHCP, select LAN 1 instead of LAN 2 at the start of the configuration procedure.

Event notification by e-mail or call home can be missing information under certain conditions

Though very unlikely, it is possible that an Event Notification by e-mail or call home may be missing information normally contained in these messages. This occurs if a switch detects an event that requires a notification to be issued, but HAFM has not completed discovery of the switch. This discovery of a switch is usually completed within a few seconds, so it is unlikely, though not impossible, that an event occurs during this short

span of time. Discovery of a switch occurs when it is added to HAFM for management, and when the Ethernet connection to a switch is broken and reestablished, such as when a switch's firmware is upgraded.

Workaround

When a switch has been added to HAFM for management, or firmware has been upgraded, observe the switch being shown as discovered by HAFM. Check the event log of the switch to ensure there were no faults that occurred during the short time when HAFM was in the process of discovering the switch.

New sound files are not added to Event Manager immediately

New sound files do not display in the pull down menu of the Event Manager. They cannot be selected for inclusion in a rule. In order for the new sound files to be available, HAFM services must be stopped and restarted, or the HAFM appliance must be rebooted. This is not disruptive to managed switches, but monitoring and logging functions are interrupted while the appliance is rebooting.

HP-UX parameters may need to be changed before you run the HAFM client

The following two HP-UX 11.0 kernel parameters are set too low for most Java applications. Usually you will see this problem as a `java.lang.OutOf MemoryError: unable to create new native thread error.` To resolve the issue, edit the following parameter limits:

- `max_thread_proc`—The maximum number of threads allowed in each process. The minimum value (and default) is `64`, which is often too low for most Java applications. Set the value of the `max_thread_proc` higher than the expected maximum number of simultaneously active threads. The maximum value is the value of `nkthread`.
- `nkthread`—The total number of kernel threads available in the system. This parameter is similar to the `nproc` tunable except that it defines the limit for the total number of kernel threads able to run simultaneously in the system. The value must be greater than nproc. The default is approximately twice that of `nproc`. The maximum is 30000. The suggested value of `nkthread` is `2*max_thread_proc`. If you have many Java processes running and each running process uses many threads, you should increase this value.

Client HAFM Login dialog box is not displayed after logging out

In some cases, when the client has logged out, the Log In dialog box is not displayed. If you get inconsistent behavior or an error message, restart the client. SAN data is not affected when you restart the client.

HAFM appliance may shut down following a firmware download

The HAFM appliance may shut down following a firmware download. If this occurs, you have to restart the HAFM appliance to recover. This is an issue with Java Virtual Machine 1.3.1_07, which is used in the application. This is only an issue when running firmware 06.00.01 or earlier.

Ethernet port on HAFM appliance may encounter problems

When you use TightVNC to access the HAFM appliance and you are running HAFM locally on the HAFM appliance, the Ethernet port on the HAFM appliance can appear to hang. When the Ethernet port encounters problems, the following may occur:

- There is an apparent loss of communication to switches being managed by HAFM.
- The appliance CPU usage and memory usage display abnormally high readings.

Workaround

If this condition persists, it may be necessary to reboot the HAFM appliance. This is not disruptive to managed switches, but monitoring and logging functions are interrupted while the appliance is rebooting.

Exporting an XML topology is not successful for all views

Exporting an XML topology only exports fabric information. For example, exporting an XML topology of a user-defined view displaying a connected set or isolated devices results in an empty XML document.